GTER 34

GTS 20

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no twitter

Ricardo Kléber Martins Galvão
www.ricardokleber.com
ricardokleber@ricardokleber.com
@ricardokleber

REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
1909-2009

GTS – 08 de Dezembro de 2012

Segurança no Twitter

Contextualizando...

Um dos pilares da **Web 2.0** são os conteúdos gerados pelos usuários (*User-Generated Content*)

- Blogs
- Comentários / Avaliações
- Informações em Redes Sociais

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Twitter

O que o torna atrativo?

- Foco na Mobilidade (ideal para uso em smartphones)
- Simplicidade/agilidade (integração com SMS)
  - Limite de 140 caracteres para mensagens
- Disponibilização de API (Interface de Acesso)
  - Facilita trabalho de desenvolvedores
  - Contribui para a criação de clientes (em todas as plataformas)
- Oferta de serviços complementares
  - Buscas
  - Estatísticas
  - Etc...

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Twitter em Números

O que o torna atrativo?

- 5 Anos de Operação

- 500 Milhões de Contas Cadastradas

(Fonte: Twopcharts :: Fevereiro/2012)

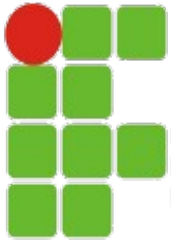
- 33,3 milhões de contas brasileiras (2° Lugar no mundo)

(Fonte: Semiocast / Janeiro/2012)

  - Na ordem: Eua / Brasil / Japão / Reino Unido / Indonésia

- 140 milhões de mensagens postadas por dia

- 1 bilhão de mensagens postadas por semana



INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Twitter

Quase todo mundo vê

Twitter

Um simples microblog...

Por que se preocupar com a **segurança** de um microblog com postagens de 140 caracteres ???

Segurança no Twitter

Por que se preocupar???

http://www.dailytech.com/LulzSec+Hacks+Apple+The+Script+Kiddies+Hack+Fox+News/article22066.htm

foxnewspolitics foxnewspolitics
We wish @joebiden the best of luck as our new President of the United States. In such a time of madness, there's light at the end of tunnel
4 Jul

foxnewspolitics foxnewspolitics
BREAKING NEWS: President @BarackObama assassinated, 2 gunshot wounds have proved too much. It's a sad 4th for #america. #obamadead RIP
4 Jul

foxnewspolitics foxnewspolitics
#ObamaDead, it's a sad 4th of July. RT to support the late president's family, and RIP. The shooter will be found
4 Jul

foxnewspolitics foxnewspolitics
@BarackObama shot twice at a Ross' restaurant in Iowa while campaigning. RIP Obama, best regards to the Obama family.
4 Jul

foxnewspolitics foxnewspolitics
@BarackObama has just passed. Nearly 45 minutes ago, he was shot twice in the lower pelvic area and in the neck; shooter unknown. Bled out
4 Jul

foxnewspolitics foxnewspolitics
@BarackObama has just passed. The President is dead. A sad 4th of July, indeed. President Barack Obama is dead

- *Agência de Notícias*
- *170.000 seguidores*
- *Morte do Presidente*
- *Dia da Independência*

04/07/2011

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no Twitter

Por que se preocupar???

http://www.pcworld.com/article/239807/anonymous_supporters_claim_nbc_news_twitter_hack.html

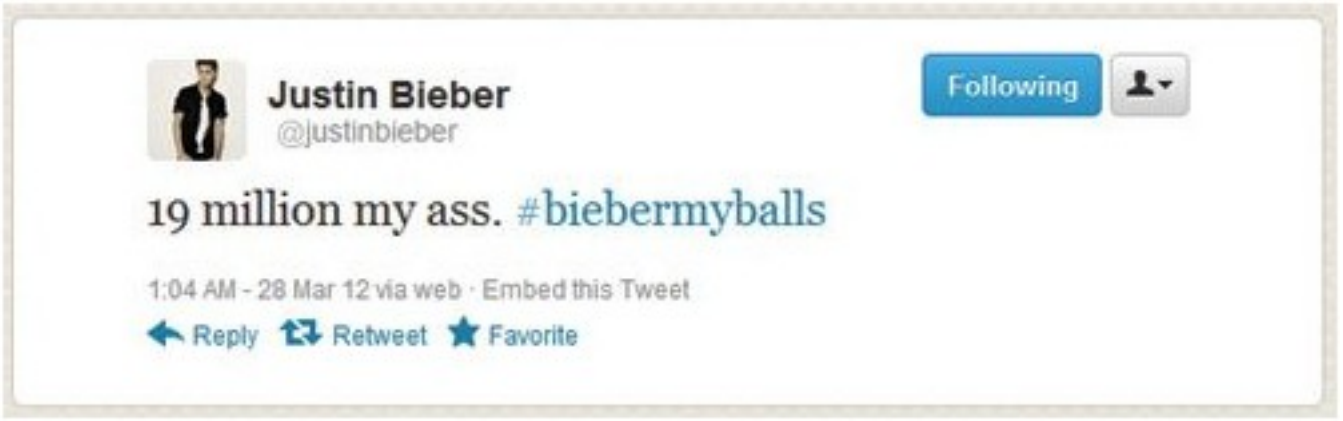
- *Agência de Notícias*
- *425.000 seguidores*
- *Notícia de Terrorismo*
- *2 Dias antes do 11/09*

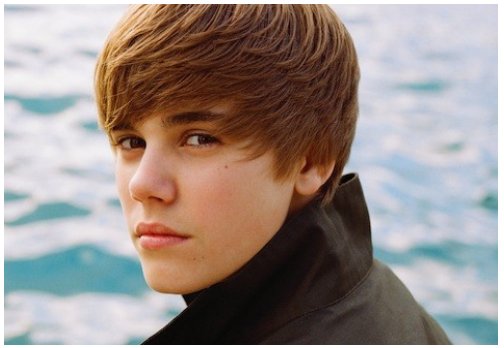
09/09/2011

Segurança no Twitter

Por que se preocupar???

http://www.zdnet.com/blog/security/justin-biebers-twitter-account-hacked/11135





- *"Astro" Pop*
- *31.000.000 seguidores*
- *Frase "ofensiva" !!??*
- *Comoção Internacional*

28/03/2012

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

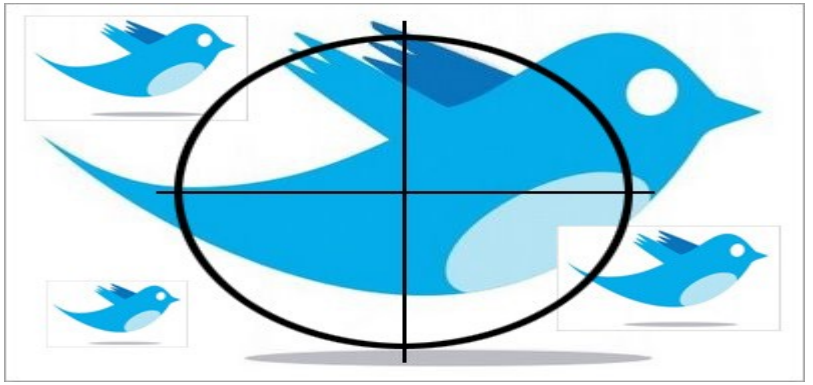
Segurança no Twitter

Por que se preocupar???

Dalai Lama

Will Smith

Steve Jobs



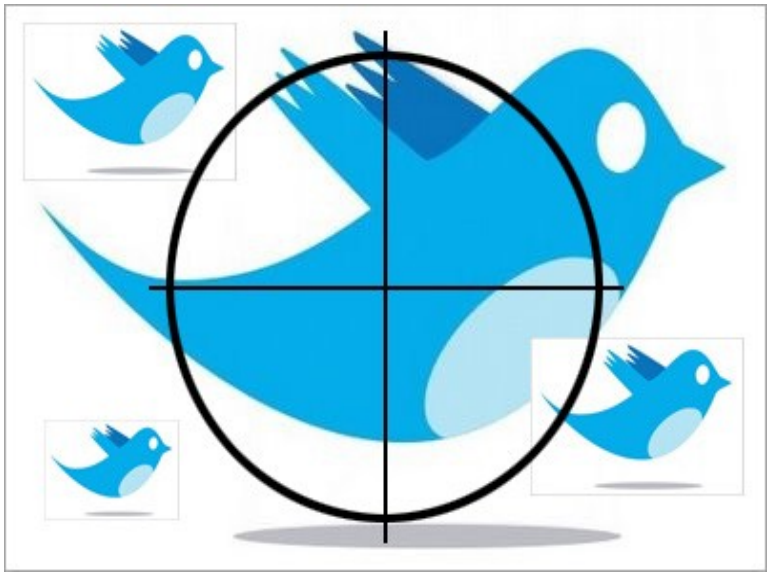
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no Twitter

Uma Comparação...

Defacement

≅



Twitter Hacking

- Foco: Imagem *(visibilidade)*
- Potencial maior *(não sujeito a visualização (enquanto "está no ar")...*

Segurança no Twitter

Onde está o Elo Mais Fraco?

- Autenticação
  - *Métodos utilizados para conexão do usuário no serviço*
- Uso de Criptografia
  - *Proteção de dados em todas as fases da comunicação*
- Armazenamento de Senhas
  - *Como os clientes guardam as informações dos usuários*

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no Twitter
Autenticação

- Identificação do Usuário `[Profile]` (login/senha)

  Dois Cenários:

  * Interface Web Oficial `(www.twitter.com)`

  * API do Twitter disponível para desenvolvedores de aplicações

Qual o percentual de utilização de Aplicativos "não oficiais"?

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança no Twitter

Autenticação

78% dos usuários do Twitter utilizam aplicações

diferentes da Interface Web Oficial

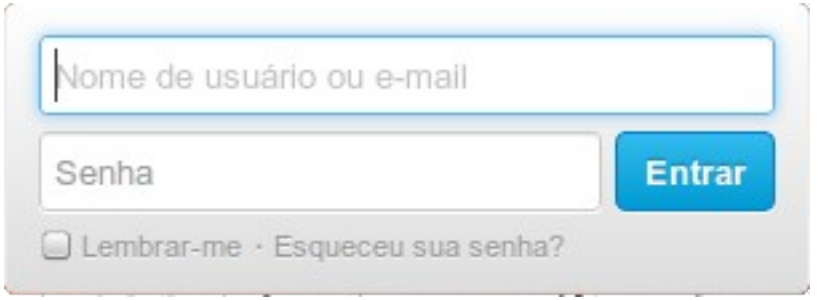
http://www.twitstat.com/twitterclientusers.html

Segurança no Twitter
Autenticação

Autenticação na Interface Web Oficial

- Usuário informa no formulário o login e a senha
- Servidor Twitter checa credenciais
- Credenciais corretas → Servidor envia token/cookie ao usuário

  (token/cookie = string randômica que identifica a sessão)
- Browser armazena cookie e envia a cada operação



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança no Twitter
Autenticação

Autenticação na Interface Web Oficial

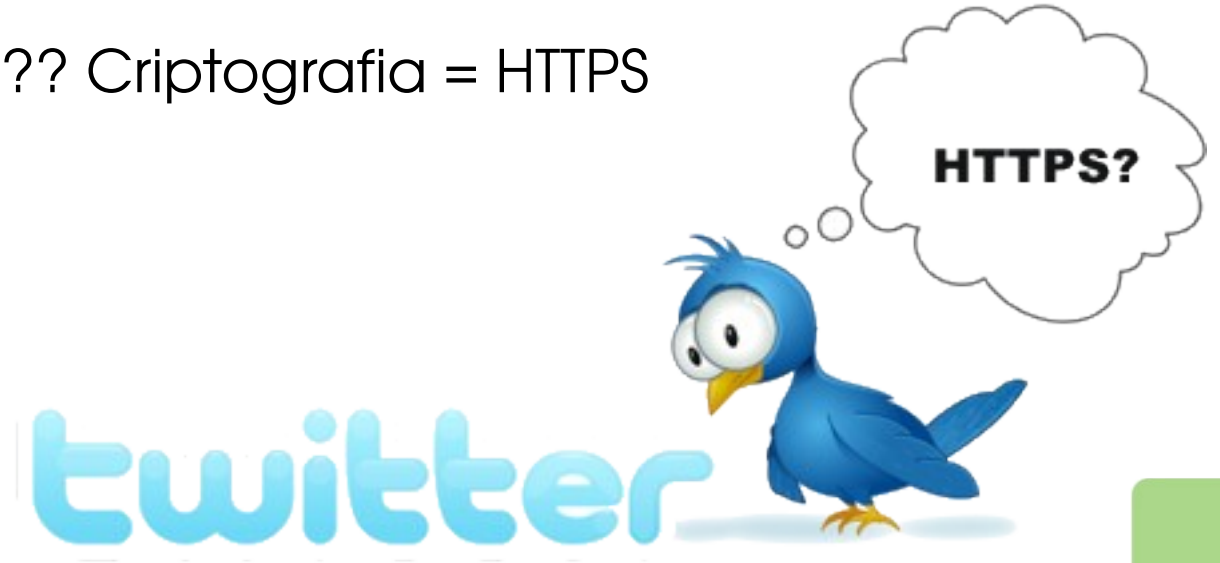
- Após a verificação inicial de credenciais...
  - Envio do cookie → Aceitação como sessão autenticada
- E se alguém "obtiver" esse cookie, preparar e enviar uma requisição (incluindo o cookie)?
  - Servidor interpreta como usuário legítimo
  - Prática conhecida como "sequestro" (hijacking) de sessão

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no Twitter
Autenticação

Autenticação na Interface Web Oficial

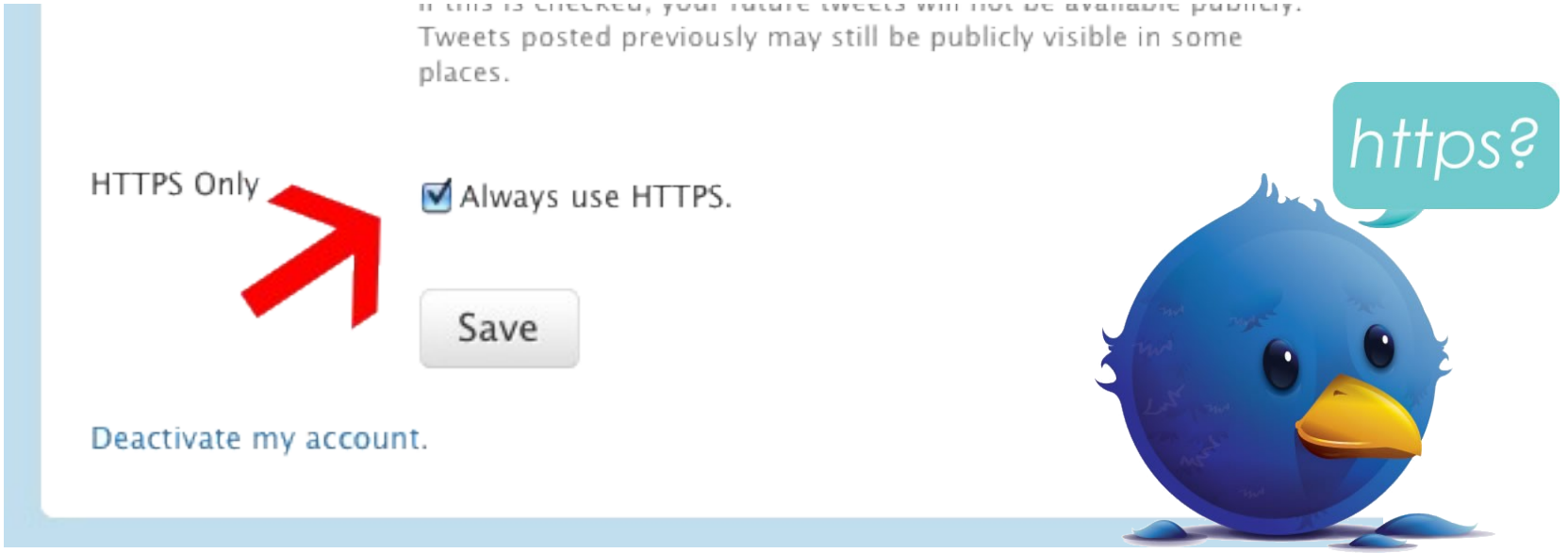
- Possibilidade de Sequestro de Sessão
  - Crítico nos primeiros anos do Twitter
  - Possibilidade real de captura de credenciais (autenticação)
  - Possibilidade real de captura de cookies
  - Solução !!?? Criptografia = HTTPS



Segurança no Twitter

Interface Web Oficial :: Uso do HTTPS

- Disponibilização (**opcional**) em 03/2011



- Modo **obrigatório** a partir de 08/2011

Segurança no Twitter
Autenticação

Autenticação em Aplicativos (uso da API do Twitter)

- Autenticação Básica (Basic Authentication)
  - *Envio de credenciais no cabeçalho de requisições http*
  - *Método **abandonado** desde setembro/2010*
- OAuth (protocolo aberto de autenticação)
  - *Método **disponibilizado** (e **sugerido**) pelo Twitter a partir de Julho/2009.*

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no Twitter

Autenticação via API do Twitter

Autenticação Básica (Basic Authentication)

- Quem utiliza(va) (Novembro/2009) *(INTECO = cert.inteco.es)*

- **TweetDeck** (v 0.31) (13,23% usuários)
- **Seesmic** (v 0.66) (4,22% usuários)
- **HootSuite** (v 03/2009) (3,32% usuários)
- **Echofon** (v 2.1) (3,11% usuários)
- **FriendFeed** (v 03/2009) (1,9% usuários)
- **Ping.fm** (v 03/2009) (1,35% usuários)
- **Twitpic** (v 03/2009) (1,35% usuários)
- **Bit.ly** (v 03/2009) (1,3% usuários)
- **Twitterrific** (v 3.2) (1,2% usuários)
- **Mobypicture** (v 03/2009) (1% usuários)
- **TwitterBerry** (v 0.9) (0,7% usuários)
- **Twdroid** (v 2.7) (0,65% usuários)

OAuth → **TwitMeme** | **Qtwitter**

Segurança no Twitter

Autenticação com uso da API do Twitter

O Que é OAuth ???

OAuth (Open Authorization) é um padrão aberto que permite que os usuários compartilhem dados entre sites/aplicações sem a necessidade de usar suas credenciais (usuário/senha). Ele se baseia no uso de tokens, que transitam entre os sites, permitindo acesso a recursos especificos.

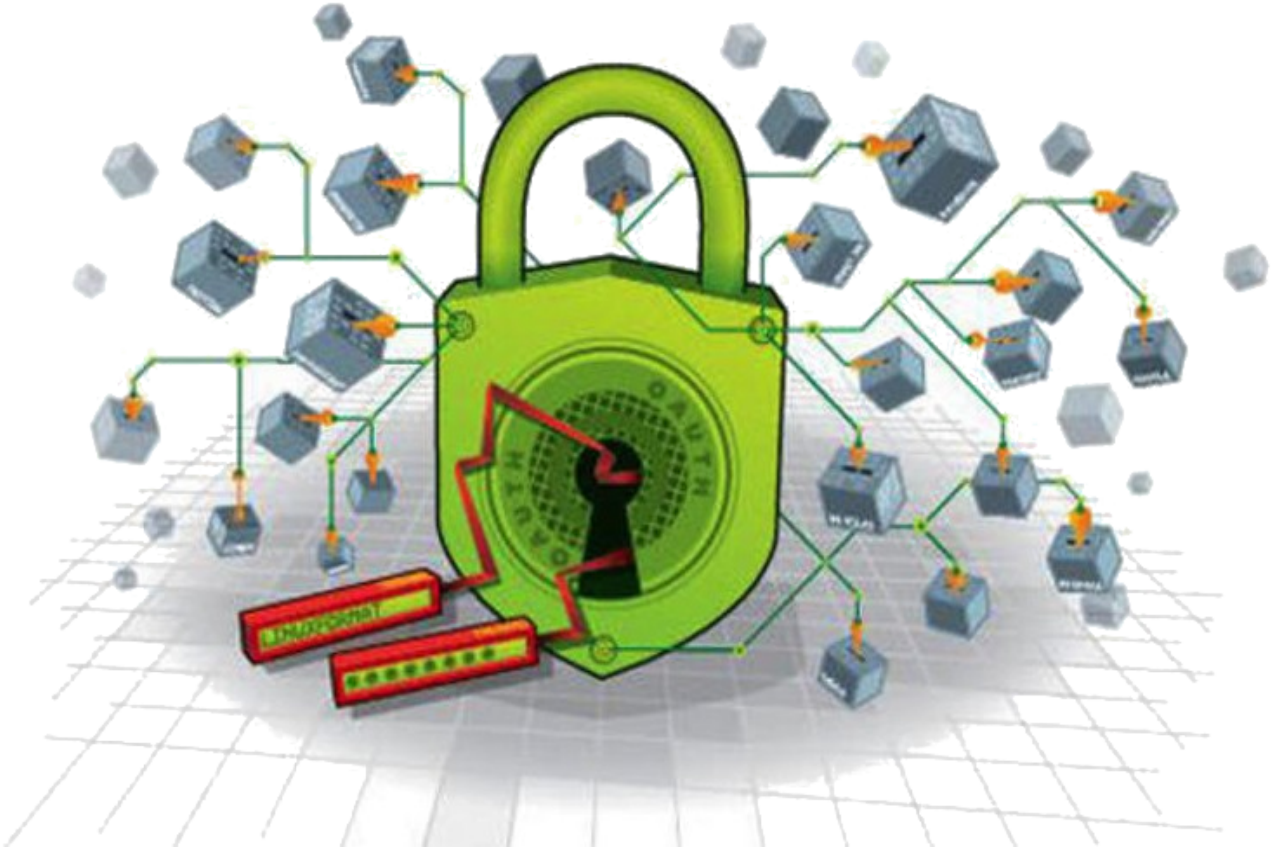
- Ensaios: Novembro/2006
  - *Blaine Cook (trabalhando na época no Twitter OpenID)*
  - *Evento: OpenID CitizenSpace*
    - *Blaine Cook / Chris Messina / David Recordon / Larry Halff*
- Abril/2007
  - *Google Group criado (proposta de protocolo aberto)*
    - *DeWitt Clinton (Google) entrou no grupo*

Versão 1.0 → 03/10/2007

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança no Twitter

Autenticação com uso da API do Twitter



Protocolo OAuth 1.0

- RFC 5849
- Abril/2010
- Working Group IETF

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no Twitter

Autenticação com uso da API do Twitter

Como Funciona o OAuth (na autenticação do Twitter) ???

- O Usuário solicita acesso à sua conta no Twitter via Aplicação (Cliente)
- A Aplicação requisita ao Twitter autorização para intermediação
- A Aplicação redireciona o usuário ao site oficial do Twitter para que seja autorizada a intermediação.
- O Usuário confirma a permissão de acesso à sua conta pela Aplicação

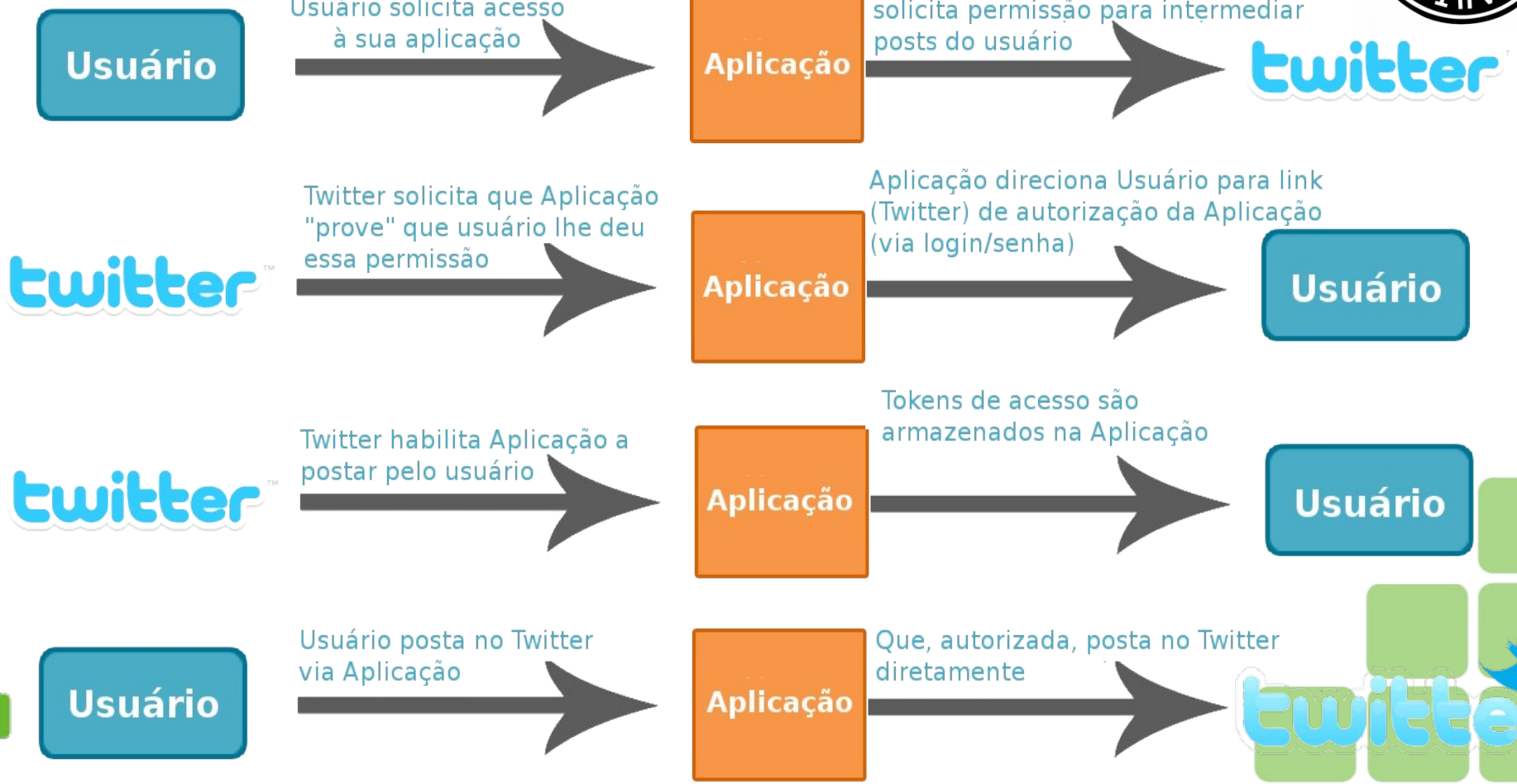
Credenciais do Usuário não trafegam na rede a cada requisição

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no Twitter

Autenticação com uso da API do Twitter

Como Funciona o OAuth ???



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no Twitter

Autenticação via API do Twitter

E Criptografia na Comunicação (SSL)?

- Quem utiliza(va) (Novembro/2009) *(INTECO = cert.inteco.es)*

- **TweetDeck** (v 0.31) **(SIM)**
- **Seesmic** (v 0.66) **(SIM)**
- **HootSuite** (v 03/2009) **(NÃO)**
- **Echofon** (v 2.1) **(SIM)**
- **FriendFeed** (v 03/2009) **(SIM)**
- **Ping.fm** (v 03/2009) **(Opcional)**

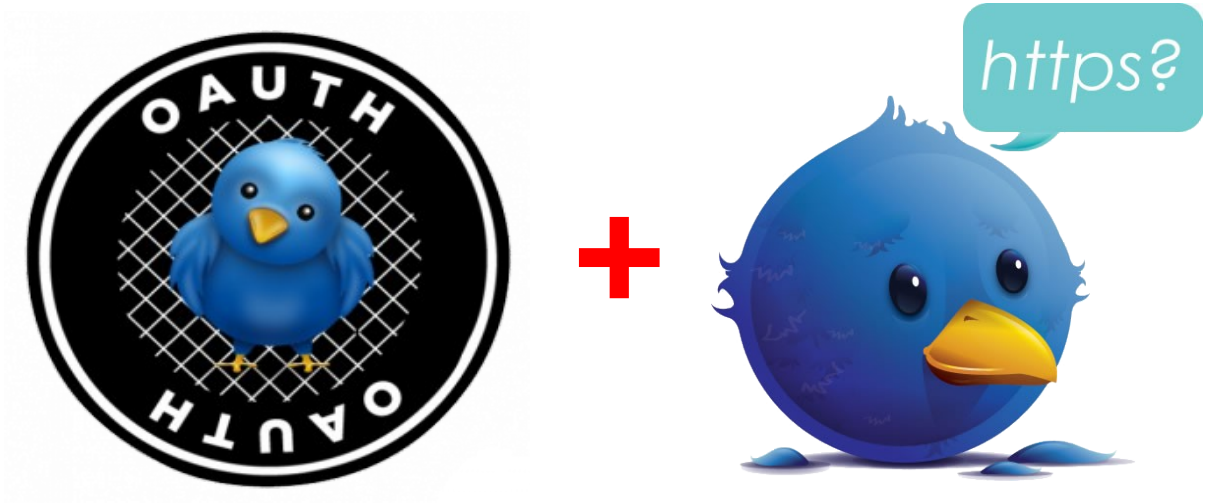
- **Twitpic** (v 03/2009) **(Opcional)**
- **Bit.ly** (v 03/2009) **(NÃO)**
- **Twitterrific** (v 3.2) **(SIM)**
- **Mobypicture** (v 03/2009) **(NÃO)**
- **TwitterBerry** (v 0.9) **(SIM)**
- **Twdroid** (v 2.7) **(SIM)**

OAuth → **TwitMeme (NÃO)** | **Qtwitter (SIM)**

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança no Twitter

Autenticação via API do Twitter



Resolve (!!??) o problema da Autenticação

- **OAuth** → **Obrigatório** desde 08/2010
- **HTTPS** → **Obrigatório** desde 08/2011

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no Twitter
Autenticação via API do Twitter

Detalhes da Autenticação baseada no OAuth

- Após autorizada, aplicação tem autonomia para postar pelo usuário (até que autorização seja revogada)
- No Twitter a autenticação de Aplicativos baseia-se em:
  - **`Consumer_Key / Consumer_Secret`** (chaves da aplicação)
  - **`OAuth_Token / OAuth_Token Secret`** (tokens do cliente)
- Chaves armazenadas (embutidas) na Aplicação/Cliente

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Detalhes da Autenticação baseada no OAuth

- Outros parâmetros utilizados no processo:

- **`oauth_nonce:`** chave aleatória gerada no processo de requisição do token.
- **`oauth_callback:`** URL p/redirecionamento após obter token de requisição.
- **`oauth_version:`** versão do OAuth a ser usado (1.0, 1.0a ou 2.0)
- **`oauth_signature_method:`** método de criptografia para a assinatura.
  (atualmente o Twitter suporta apenas HMAC-SHA1)
- **`oauth_timestamp:`** timestamp atual, em formato Unix

Segurança no Twitter
Autenticação via API do Twitter

Detalhes da Autenticação baseada no OAuth

- Outros parâmetros utilizados no processo:

- **`oauth_signature:`** assinatura gerada a partir da concatenação do método de requisição com a URL requisitada e os parâmetros passados, em ordem alfabética.
- **`oauth_token:`** token de requisição, reenviado para a URL de retorno.
- **`oauth_verifier:`** código verificador, gerado pela autorização do usuário.

Segurança no Twitter
Autenticação via API do Twitter

- Alguns bugs/problemas de segurança reportados:

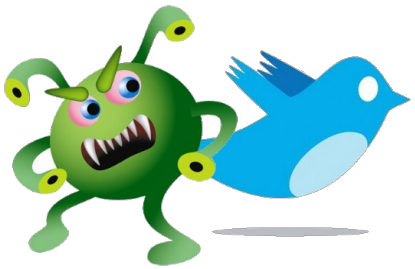
- **Divulgação Pública de `Consumer_Key / Consumer Secret`**
  - Revogação da Autorização da Aplicação/Cliente
  - Necessidade de Novo Registro da Aplicação/Cliente
  - Impossibilidade de Uso pelo Usuário até upgrade de versão
  - Técnica pode ser utilizada por "concorrentes"
  - `Astro → TwitterApp → SD Card → Pacote APK → classes.dex → strings/grep`
  - Aplicações/Clientes Open Source criticamente vulneráveis
- **Uso de chaves sequestradas/descobertas para spam/phishing**
  - Ação antes da revogação das chaves
- **`oauth_timestamp:`** Autenticação falha se relógio do usuário estiver atrasado
  - API nega autenticação de requisições com timestamp anteriores ao timestamp da última requisição.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança no Twitter
Autenticação via API do Twitter

- Alguns bugs/problemas de segurança reportados:

- **`oauth_callback:`** Aplicação Maliciosa pode informar como URL de redirecionamento uma página falsa (Twitter Fake Page) para capturar Credenciais (login/senha) do Usuário.
- **`oauth_version:`** Twitter não suporta versão 2.0



Estes e outros alertas sobre segurança no uso do protocolo OAuth pelo Twitter:

- **Compromising Twitter's OAuth Security System**
  - **Ryan Paul** *(desenvolvedor do Gwibber = Cliente Twitter)*
  - `Arstechnica.com`

Segurança no Twitter

Armazenamento das Senhas/Tokens

Aplicativos usam criptografia para **armazenar** senhas/tokens?

- Quem utiliza(va) (Novembro/2009) *(FINTECO = cert.inteco.es)*

- **TweetDeck** (v 0.31) **(SIM)**
- **Seesmic** (v 0.66) **(SIM)**
- **Echofon** (v 2.1) **(SIM)**
- **Twitterrific** (v 3.2) **(SIM)**
- **Mobypicture** (v 03/2009) **(SIM)**
- **TwitterBerry** (v 0.9) **(SIM)**
- **Twdroid** (v 2.7) **(SIM)**
- **TinyTwitter** (v 1.8) **(NÃO)** **(0,1% usuários)**

Aplicações que utilizam plataforma WEB não foram consideradas para essa análise

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no Twitter

O Que vem por aí...

Framework OAuth 2.0

- RFC 6749
- Outubro/2012
- Working Group IETF
- Facebook API suporte exclusivo
- Google e Microsoft (suporte experimental)
- Exclusivo: Bearer Token (RFC 6750)
  - Não suporta outro tipo de mecanismo de assinatura, criptografia e verificação de cliente.

Segurança no Twitter

Panorama de Uso do OAuth

- **Dropbox** :: OAuth 1.0
- **Facebook** :: OAuth 2.0 (draft)
- **Flickr** :: OAuth 1.0a
- **Foursquare** :: OAuth 2.0
- **Google** :: OAuth 2.0
- **Instagram** :: OAuth 2.0
- **Microsoft** :: OAuth 2.0

  (Hotmail, Windows Live, Messenger, Xbox)
- **LinkedIn** :: OAuth 1.0a
- **MySpace** :: OAuth 1.0a
- **Netflix** :: OAuth 1.0a
- **Paypal** :: OAuth 2.0
- **Twitter** :: OAuth 1.0a
- **Yahoo!** :: OAuth 1.0a

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Segurança no Twitter

OAuth 2.0 :: Polêmica...

"Comparando o OAuth 2.0 com a versão anterior, ele é mais complexo, menos interoperável, menos útil, mais incompleto e... mais importante: menos seguro"

Eran Hammer

(ex-Líder do Projeto OAuth 2.0)

Abandonou o projeto em Julho/2012
por não concordar com os rumos tomados

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Perguntas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

GTER 34

GTS 20

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Segurança no twitter

Ricardo Kléber Martins Galvão
www.ricardokleber.com
ricardokleber@ricardokleber.com
@ricardokleber

REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
1909-2009

GTS – 08 de Dezembro de 2012